Чернівецький національний університет імені Юрія Федьковича

(повне найменування закладу вищої освіти)

Навчально-науковий інститут фізико-технічних і комп'ютерних наук

(назва інституту/факультету)

Кафедра комп'ютерних систем та мереж

(назва кафедри)

СИЛАБУС

навчальної дисципліни

Технологія IoT Blockchain

(вкажіть назву навчальної дисципліни (іноземною, якщо дисципліна викладається іноземною мовою))

вибіркова

(обов'язкова чи вибіркова)

Освітньо-професійна програма – *" Комп'ютерна інженерія "*

Спеціальність *123 – Комп'ютерна інженерія*

(шифр і назва спеціальності)

Галузь знань *12 – Інформаційні технології*

(шифр і назва галузі знань)

Рівень вищої освіти – *другий (магістерський)*

(вказати: перший (бакалаврський)/другий (магістерський)/третій (освітньо-науковий))

Навчально-науковий інститут фізико-технічних і комп'ютерних наук

(назва факультету / інституту, на якому здійснюється підготовка фахівців за вказаною освітньо-професійною програмою)

Мова навчання – *українська*

(мова, на якій читається дисципліна)

Розробники: Іванущак Наталія Михайлівна, асистент кафедри КСМ, кандидат техн. наук,

(вказати авторів (викладач (ів)), їхні посади, наукові ступені, вчені звання)

Профайл викладача (-ів) https://csn.chnu.edu.ua,
https://csn.chnu.edu.ua/employees/ivanushhak-nataliya-myhajlivna/

Контактний тел. +(38) 0372 50 94 32 (кафедра КСМ) – Іванущак Н.М.

E-mail: n.ivanuschak@chnu.edu.ua

Сторінка курсу в мережній академії Cisco https://lms.netacad.com/course/view.php?id=1509455

Консультації *on-line: середа з 17.00 до 18.00*

1. Анотація дисципліни

Курс «Технологія IoT Blockchain» призначений для розширення компетентностей випускників спеціальності 123 - Комп'ютерна інженерія для набуття студентами базових знань побудови системи зі здійснення фінансових мікротранзакцій між цифровими об’єктами підключених пристроїв IoT.

Вивчення даної вибіркової дисципліни надає студентам ряд переваг, оскільки матеріал курсу допоможе при аналізі інформаційних джерел, підготовці магістерських робіт, статей, доповідей на науково-практичних конференціях. Окрім цього, засвоєння дисципліни дозволить майбутнім фахівцям забезпечити необхідний рівень володіння інструментами дослідження і проектування комплексної системи захисту інформації, в тому числі комерційного характеру.

2. Мета навчальної дисципліни: надання студентам міждисциплінарних знань для побудови системи міжмашинної взаємодії пристроїв Інтернету речей та створення машинно-машинної (M2M) економіки – що, по суті, є обміном грошима між пристроями і вилучення людини із процесу їх взаємодії і функціонування.

3. Пререквізити. Для коректного розуміння і засвоєння матеріалу даного курсу слухачі повинні попередньо пройти курси: криптографія та побудова систем безпеки, захист інформації в комп’ютерних системах, комп’ютерні мережі, основи баз даних. Доцільно також мати певні уявлення з архітектури комп’ютерів, комп’ютерної схемотехніки, програмування.

4. Результати навчання

У результаті вивчення навчальної дисципліни студент повинен

4.1. Знати: найновіші досягнення в галузі інформаційної безпеки банківського бізнесу, наявні існуючі системи здійснення мікроплатежів, системи міжмашинної взаємодії (M2M), основи технології блокчейн, принципи формування блокчейн-мереж, основи побудови захищених систем Інтернету речей та мереж блокчейн, контроль та моніторинг цих систем.

4.2. Вміти: будувати системи Інтернету речей із врахуванням вимог кібербезпеки для їх подальшого масштабування та підвищення продуктивності для побудови машинно-машинної (M2M) економіки - цифрових грошей для мікротранзакцій; обирати для проектування криптовалютні проекти, орієнтованих на індустрію Інтернету речей; будувати розподілені мережі Інтернету речей для керування, моніторингу та управління; забезпечувати підвищений рівень захисту побудованих систем.

4.3. Набути компетентностей:

ЗК - загальних

ЗК3. Здатність проводити дослідження на відповідному рівні.

ЗК4. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.
ЗК6. Здатність виявляти, ставити та вирішувати проблеми.
ЗК7. Здатність приймати обґрунтовані рішення.

СК – фахових (спеціальних)

СК1. Здатність до визначення технічних характеристик, конструктивних особливостей, застосування і експлуатації програмних, програмно-технічних засобів, комп'ютерних систем та мереж різного призначення.
СК3. Здатність проектувати комп'ютерні системи та мережі з урахуванням цілей, обмежень, технічних, економічних та правових аспектів.
СК4. Здатність будувати та досліджувати моделі комп'ютерних систем та мереж.
СК5. Здатність будувати архітектуру та створювати системне і прикладне програмне забезпечення комп'ютерних систем та мереж.
СК6. Здатність використовувати та впроваджувати нові технології, включаючи технології розумних, мобільних, зелених і безпечних обчислень, брати участь в модернізації та реконструкції комп'ютерних систем та мереж, різноманітних вбудованих і розподілених додатків, зокрема з метою підвищення їх ефективності.
СК7. Здатність досліджувати, розробляти та обирати технології створення великих і надвеликих систем.
СК8. Здатність забезпечувати якість продуктів і сервісів інформаційних технологій на протязі їх життєвого циклу.
СК10. Здатність ідентифікувати, класифікувати та описувати роботу програмно-технічних засобів, комп'ютерних систем, мереж та їхніх компонентів.

ПРН - програмних результатів навчання

РН2. Знаходити необхідні дані, аналізувати та оцінювати їх.
РН3. Будувати та досліджувати моделі комп'ютерних систем і мереж, оцінювати їх адекватність, визначати межі застосовності.
РН4. Застосовувати спеціалізовані концептуальні знання, що включають сучасні наукові здобутки у сфері комп'ютерної інженерії, необхідні для професійної діяльності, оригінального мислення та проведення досліджень, критичного осмислення проблем інформаційних технологій та на межі галузей знань.
РН7. Вирішувати задачі аналізу та синтезу комп'ютерних систем та мереж.
РН11. Приймати ефективні рішення з питань розроблення, впровадження та експлуатації комп'ютерних систем і мереж, аналізувати альтернативи, оцінювати ризики та імовірні наслідки рішень.

5. Опис навчальної дисципліни
5.1. Загальна інформація

Назва навчальної дисципліни *Технологія IoT Blockchain*												
Форма навчання	**Рік підготовки**	**Семестр**	**Кількість**			**Кількість годин**						**Вид підсум-кового контролю**
			кредитів	**годин**	**змістових модулів**	**лекції**	**практичні**	**семінарські**	**лабораторні**	**самостійна робота**	**індивідуальні завдання**	
Денна	**1(5)**	**1(9)**	**4**	**120**	**2**	**15**	**-**	**-**	**15**	**90**	**-**	**Залік**
Заочна	**1(5)**	**1(9)**	**4**	**120**	**2**	**4**	**-**	**-**	**4**	**112**	**-**	**Залік**

Примітка. Співвідношення кількості годин аудиторних занять до самостійної і індивідуальної роботи становить: для денної форми навчання – 0,33 ((15+15)/90);
для заочної форми навчання – 0,07 ((4+4)/112).

5.2. Дидактична карта навчальної дисципліни

Назви змістових модулів і тем	Кількість годин											
	Денна форма						Заочна форма					
	усього	у тому числі					усього	у тому числі				
		л	п	лаб	інд	с.р.		л	п	лаб	інд	с.р.
1	2	3	4	5	6	7	8	9	10	11	12	13
Змістовий модуль 1. Блокчейн та Інтернет речей (IoT)												
Тема 1. Вступ. Основні поняття побудови екосистеми Інтернету речей.	14	2	-	2	-	10	14	1	-	1	-	12
Тема 2. Аналіз моделі загроз для системи IoT	14	2	-	2	-	10	14	0	-	-	-	14
Тема 3. Основи технології блокчейн	14	2	-	2	-	10	16	1	-	1	-	14
Тема 4. Система блокчейн для побудови машинно-машинної (M2M) економіки.	14	2	-	2	-	10	16	0	-	-	-	16
Разом за змістовим модулем 1	56	8	-	8	-	40	60	2	-	2	-	56
Змістовий модуль 2. Механізми захисту мереж Інтернету речей												
Тема 5. Захист Інтернету речей на рівні пристроїв.	19	2	-	2	-	15	20	1	-	1	-	18
Тема 6. Захист Інтернету речей на рівні комунікацій.	19	2	-	2	-	15	18	0	-	-	-	18
Тема 7. Захист Інтернету речей на рівні додатків.	26	3	-	3	-	20	22	1	-	1	-	20
Разом за змістовим модулем 2	64	7	-	7	-	50	60	2	-	2	-	56
Усього годин	120	15	-	15	-	90	120	4	-	4	-	112

5.3. Тематика лабораторних занять

№	Назва теми (завдання)	Кількість годин
1.	Дослідження IoT системи розумний дім	2
2.	Налаштування міжмашинної взаємодії в IoT системі	2
3.	Моделювання загроз на рівні пристроїв Інтернету речей	2
4.	Моделювання загроз на комунікаційному рівні IoT	2
5.	Моделювання загроз на прикладному рівні IoT	3
6.	Моделювання загроз для оцінки ризиків у системі IoT	3
7.	Побудова захищеної системи мікроплатежів IoT-системи за допомогою блокчейн	3
	Разом	15

Примітка. Методичні рекомендації та завдання до лабораторних робіт доступні на інтернет-ресурсі Академії CISCO IoT Fundamentals: IoT Security**:**
https://www.netacad.com/courses/cybersecurity/iot-security

Програмне забезпечення для виконання лабораторних робіт: середовище програмування Cisco Packet Tracer.

5.4. Зміст завдань для самостійної роботи

№ з/п	**Назва теми**	**Кількість годин**
1	Чому блокчейн потребує масштабування?	10
2	Стейкінг (Proof of Stake)	10
3	Майнінг (Proof of Work)	10
4	Блокчейн та розподілені файлові системи	15
5	Анатомія атаки IoT	15
6	Моделі контролю доступу	15
7	Керування ідентифікацією пристроїв IoT	15
	Разом	90

6. Система контролю та оцінювання

Засобами оцінювання та демонстрування результатів навчання є

- контрольні роботи;
- стандартизовані тести;
- презентації результатів виконаних завдань та досліджень;
- завдання на лабораторному обладнанні.

Формами поточного контролю рівня знань є усна та письмова відповідь студента при захисті виконаних лабораторних робіт, кількість отриманих балів при виконанні тестового завдання, а також письмова відповідь при написанні модульних контрольних робіт. Формами підсумкового контролю рівня знань є виконання підсумкового тестування.

6.1. Критерії оцінювання результатів навчання з навчальної дисципліни

Критерієм успішного проходження здобувачем освіти підсумкового

оцінювання є досягнення ним мінімальних порогових рівнів оцінок за кожним запланованим результатом навчання навчальної дисципліни.

Шкала оцінювання: національна та ЄКТС (Європейська кредитна трансферно-накопичувальна система, ECTS)

Оцінка за національною шкалою (залік)	Оцінка за шкалою ЄКТС	
	Оцінка (бали)	**Пояснення за розширеною шкалою**
Зараховано	A (90-100)	Зараховано
	B (80-89)	
	C (70-79)	
	D (60-69)	
	E (50-59)	
Не зараховано	FX (35-49)	Не зараховано з можливістю повторного складання
	F (1-34)	Не зараховано з обов'язковим повторним вивченням дисципліни

Розподіл балів, які отримують студенти

Поточне тестування та самостійна робота									Підсумковий тест (залік)	Сума балів
Змістовий модуль 1					Змістовий модуль 2				30	100
Т1	Т2	Т3	Т4	М1	Т5	Т6	Т7	М2		
5	5	5	5	10	10	10	10	10		

6.2. Перелік тем і розподіл максимально можливої кількості балів, які отримують студенти за виконання всіх видів навчальної діяльності

Змістовий модуль 1. Блокчейн та Інтернет речей (IoT)

Т1. Вступ. Основні поняття побудови екосистеми Інтернету речей (виконання та захист лабораторної роботи №1 на основі лекційного матеріалу та методичних вказівок до лабораторної роботи – 5 балів).

Т2. Аналіз моделі загроз для системи IoT (виконання та захист лабораторної роботи № 2 на основі лекційного матеріалу та методичних вказівок до лабораторної роботи – 5 балів).

Т3. Основи технології блокчейн (виконання та захист лабораторної роботи № 3 на основі лекційного матеріалу та методичних вказівок до лабораторної роботи – 5 балів).

Т4. Система блокчейн для побудови машинно-машинної (M2M) економіки (виконання та захист лабораторної роботи № 4 на основі лекційного матеріалу та методичних вказівок до лабораторної роботи – 5 балів).

М1 – модульна контрольна робота №1 (10 балів)

Змістовий модуль 2. Механізми захисту мереж Інтернету речей

Т5. Захист Інтернету речей на рівні пристроїв (виконання та захист лабораторної роботи № 5 на основі лекційного матеріалу та методичних вказівок до лабораторної роботи – 10 балів).

Т6. Захист Інтернету речей на рівні комунікацій (виконання та захист лабораторної роботи № 6 на основі лекційного матеріалу та методичних вказівок до лабораторної роботи – 10 балів).

Т7. Захист Інтернету речей на рівні додатків (виконання та захист лабораторної роботи № 7 на основі лекційного матеріалу та методичних вказівок до лабораторної роботи – 10 балів).

М2 – модульна контрольна робота №2 (10 балів).

Підсумковий контроль (**залік**) – 30 балів: здійснюється виконання фінальної контрольної роботи на курсі Академії CISCO IoT Fundamentals: IoT Security. **Сумарна кількість балів** – 100.

6.3. Умови зарахування результатів неформальної освіти

Студент, згідно Положення ЧНУ «Про неформальну освіту» може отримати додаткові бали, або бути звільненим від окремих видів роботи з окремих тем, якщо у нього наявні сертифікати про неформальну освіту з проблем, які вивчаються на дисципліні «Комп'ютерні системи штучного інтелекту».

Також, як виконані види роботи з відповідних тем зараховуються студенту бали за наукові публікації у матеріалах науково-практичних конференцій та фахових чи апробаційних виданнях.

7. Рекомендована література

Фахова (основна)

1. Дудатьєв А. В. Захист комп'ютерних мереж. Теорія та практика. Навчальний посібник / Дудатьєв А. В., Войтович О. П., Каплун В. А.- Вінниця ВНТУ, 2010.-219 с.
2. IoT maturity in the new digital world URL: https://internetofthingsagenda.techtarget.com/blog/IoT-Agenda/Get-smart-about-data-integration-for-a-truly-smart-city
3. IT Strategy Headquarters. «E-Japan Strategy» January 22, 2001 URL: https://japan.kantei.go.jp/it/network/0122full_e.html
4. Яцків Н. Г. Перспективи використання технології блокчейн у мережі інтернет речей . Науковий вісник НЛТУ України. 2016. Вип. 26.8. С. 381-387. [Електронний ресурс]. URL: http://nbuv.gov.ua/UJRN/nvnltu_2016_26.

Допоміжна

1. Мельник А. О. Кіберфізичні системи: проблеми створення та напрями розвитку. Вісник Національного університету "Львівська політехніка". 2014. № 806 : Комп'ютерні системи та мережі. С. 154–161.
2. Наконечний А.Й., Верес З.Є. Інтернет речей і сучасні технології. Вісник Національного університету "Львівська політехніка". Автоматика, вимірювання та керування. 2016. № 852.С. 136-138.

3. Roundup Of Internet Of Things Forecasts 2017. [Electronic resource]. URL: https://www.forbes.com/sites/louiscolumbus/2017/12/10/2017-roundup-of-internet-of-thingsforecasts/#77a4556b1480.

8. Інформаційні ресурси

1. https://csn.chnu.edu.ua/about-us/ok-rivni/
2. https://csn.chnu.edu.ua/spetsialnist-123-komp-yuterna-inzheneriya-opp-komp-yuterna-inzheneriya-magistratura-1-5-r/

3. Cisco -Україна. Режим доступу:: https://www.cisco.com
4. Annual Threat Reports. Режим доступу:: https://www.fireeye.com/current-threats/annual-threat-report.html
5. European union agency for cybersecurity. Режим доступу:: https://www.enisa.europa.eu
6. IoT Fundamentals: IoT Security. Інтернет-ресурс Академії CISCO, Режим доступу: https://www.netacad.com/courses/cybersecurity/iot-security